METHOD, SYSTEM AND TERMINAL DEVICE FOR SCANNING VIRUS

Abstract: A method, a system and a terminal device for virus scanning are described and related to the field of Internet technology. The method includes: monitoring whether a terminal device performs a lock screen operation; determining whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time; and if the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time, enabling the security software program to perform the virus scan. In the method, the system and the terminal device, a virus can be scanned in time and the efficiency of virus scanning can be relatively improved.

Published: with international search report (Art. 21(3))
METHOD, SYSTEM AND TERMINAL DEVICE FOR SCANNING VIRUS

CROSS-REFERENCE TO RELATED APPLICATIONS
This application claims the benefit of priority from Chinese Patent Application No. 201310208250.X, and filed on May 30, 2013, the content of which is hereby incorporated in its entirety by reference.

FIELD
The disclosure relates to the field of internet technology, and particularly to a method, a system and a terminal device for scanning virus.

BACKGROUND
This section provides background information related to the present disclosure which is not necessarily prior art.

More and more software appears in a smartphone with the development of the smartphone technology. However, a virus (i.e. a malware) may be installed in some percentage of the software to promote an advertisement anonymously, to download software without authority, and even to charge secretly, which becomes a potential threat by stealing network traffic or charge from the smartphone. To eliminate the threat existed in the smartphone, a security software program can be provided to perform a virus scan. While in practical applications, a user needs to enable the security software program in the smartphone in person, and needs to manually perform the virus scan to find the virus. However, in practice, the user usually performs the virus scan in a long interval. Thus, the virus cannot be scanned in time,
and an efficiency of virus scanning also can be reduced.

SUMMARY
Exemplary embodiments of the present invention provide a method, a system and a terminal device for scanning virus, in which a virus can be scanned in time and the efficiency of virus scanning can be improved.

One embodiment of the present invention provides a method for scanning virus, comprising: monitoring whether a terminal device performs a lock screen operation; if the terminal device performs the lock screen operation, determining whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time; and if the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time, enabling the security software program to perform the virus scan.

Another embodiment of the present invention provides a system for scanning virus, comprising: a monitoring unit configured to monitor whether a terminal device performs a lock screen operation; a first determining unit configured to determine whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time, when the monitoring unit detects the terminal device performs the lock screen operation; and a scan enabling unit configured to enable the security software program to perform the virus scan when the first determining unit determines that the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time.
Yet another embodiment of the present invention provides a terminal device, comprising a system for virus scanning described above.

In exemplary embodiments of the present invention, when a lock screen operation performed on a terminal device is detected, it can be determined whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time. If the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time, the security software program can be enabled to perform the virus scan. The terminal device performs the lock screen operation automatically or under control of the user, which may cause the terminal device performing the lock screen operation frequently. Thus, when the terminal device performs the lock screen operation, it can be taken as a trigger condition. A virus can be scanned in time and an efficiency of virus scanning can be relatively improved.

**BRIEF DESCRIPTION OF THE DRAWINGS**

In order to illustrate technical solutions according to embodiments of the disclosure, a brief description of drawings that assists the description of embodiments of the invention or existing art will be provided below. It would be apparent that the drawings in the following description are only for some of the embodiments of the invention. A person having ordinary skills in the art will be able to obtain other drawings on the basis of these drawings without paying any creative work.

Fig. 1 is a flowchart of an example of a method for scanning virus according to various embodiments;
Fig. 2 is a flowchart of another example of a method for scanning virus according to various embodiments;
Fig. 3 is a structure diagram of an example of a system for scanning virus according to various embodiments;
Fig. 4 is a structure diagram of another example of a system for scanning virus according to various embodiments;
Fig. 5 is a structure diagram of an example of a terminal device according to various embodiments.

DETAILED DESCRIPTION

Technical solutions in embodiments of the present invention will be illustrated clearly and entirely with the aid of the drawings in the embodiments of the invention. It is apparent that the illustrated embodiments are only some embodiments of the invention instead of all of them. Other embodiments that a person having ordinary skills in the art obtains based on the illustrated embodiments of the invention without paying any creative work should all be within the protection scope sought by the present invention.

A method, a system and a terminal device for scanning virus disclosed in exemplary embodiments can scan a virus in time and relatively improve the efficiency of virus scanning. The illustrations for the method, the system and the terminal device will be described respectively as below.

Referring to Fig. 1, it is a flowchart of an example of a method for scanning virus according to various embodiments. The method can be applied for a terminal device such as a smart phone (e.g., an Android phone, an iOS phone, etc.), a tablet computer,
a portable computer, a mobile internet device (MID), a personal computer, and so on.

The method may include the following steps.

Step S101 is: monitoring whether a terminal device performs a lock screen operation. If the lock screen operation performed by the terminal device is detected, step S102 can be executed; if the lock screen operation performed by the terminal device is not detected, the flow may come to the end.

In one embodiment of the invention, the terminal device can perform the lock screen operation automatically or under control of the user. For example, when the user has not actively use the terminal device for 5 minutes, 10 minutes, 15 minutes, or the like, the terminal device can perform the lock screen operation automatically; or the terminal device can perform the lock screen operation when receiving the control command from the user.

Step S102 is: if the terminal device performs the lock screen operation, determining whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time. If the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time, step S105 can be executed; if the virus scan has been performed on the terminal device during the period from the time at which the security software program is installed to the current time, step S103 can be executed.

In one embodiment of the invention, the terminal device can record the time at which the security software program is installed after it may accomplish the installation of the security software program. And then, when the lock screen operation performed by the terminal device is detected, it may be determined whether the virus scan has
been performed on the terminal device during the period from the time at which the security software is installed to the current time.

Step 103 is: if determining that the virus scan has been performed on the terminal device during the period from the time at which the security software program is installed to the current time, determining whether the virus scan has been performed on the terminal device during a period from a last time at which a virus database is updated to the current time. If the virus scan has never been performed on the terminal device during the period from the last time at which the virus database is updated to the current time, step S105 can be executed; if the virus scan has been performed on the terminal device during the period from the last time at which the virus database is updated to the current time, step S104 can be executed.

In one embodiment of the invention, the terminal device can record the last time at which the virus database is updated. Then, when it is determined that the virus scan has been performed during the period from the time at which the security software program is installed to the current time, it may be determined whether the virus scan has been performed during the period from the last time at which the virus database is updated to the current time.

Step S104 is: if determining that the virus scan has been performed on the terminal device during the period from the last time at which the virus database is updated to the current time, determining whether a time interval between a last time of virus scanning and the current time is greater than or equal to a preset time threshold. If the time interval between the last time of virus scanning and the current time is greater than or equal to the preset time threshold, step S105 can be executed; if the time interval between the last time of virus scanning and the current time is less than the
preset time threshold, the flow may come to the end.

In one embodiment of the invention, the terminal device can record the last time of virus scanning. Then, when it is determined that the virus scan has been performed during the period from the last time at which the virus database is updated to the current, it may be determined whether the time interval between the last time of virus scanning and the current is greater than or equal to the preset time threshold (e.g. 1 day, 3 days, or 5 days).

Step S105 is: enabling the security software program to perform the virus scan.

In practical applications, it may consume a certain resource of the terminal device to enable the security software program to perform the virus scan. While in one embodiment of the invention, virus scanning can only be triggered at the condition when the screen of the terminal device is locked. Thus the running speed of the terminal device controlled by the user may not be influenced.

In one embodiment of the invention, the security software program can also perform the virus scan at the background, which means a security software interface may not need to be enabled. Thus, the consumed resource of the terminal device during the virus scan can be reduced; for example, the terminal device may consume power, etc.

In one embodiment of the invention, the method shown in Fig. 1 can further include the following step: outputting a virus scan result, wherein the virus scan result includes the number of viruses and a prompt message which is used to prompt operations to be performed on a virus, the operations including a clearing operation and an ignoring operation.

When the user selects the clearing operation, the terminal device may clear a detected virus; when the user selects the ignoring operation, the terminal device may ignore the
detected virus.

In exemplary embodiments of the present invention, when a lock screen operation performed on a terminal device is detected, it may be determined whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time. If the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time, the security software program can be enabled to perform the virus scan. The terminal device can perform the lock screen operation automatically or under control of the user, which may cause the terminal device performing the lock screen operation frequently. Thus, when the terminal device performs the lock screen operation, it can be taken as a trigger condition. A virus can be scanned in time and the efficiency of virus scanning can be relatively improved.

Referring to Fig. 2, it is a flowchart of another example of a method for scanning virus according to various embodiments. The method can be applied for a terminal device such as a smart phone (e.g., an Android phone, an iOS phone, etc.), a tablet computer, a portable computer, a mobile internet device (MID), a personal computer, and so on. The method may include the following steps.

Step S201 is: monitoring whether a terminal device performs a lock screen operation.

If the lock screen operation performed by the terminal device is detected, step S202 can be executed; if the lock screen operation performed by the terminal device is not detected, the flow may come to the end.

In one embodiment of the invention, the terminal device can perform the lock screen operation automatically or under control of the user. For example, when the user has
not actively use the terminal device for 5 minutes, 10 minutes, 15 minutes, or the like, the terminal device can perform the lock screen operation automatically; or the terminal device can perform the lock screen operation when receiving the control command from the user.

Step S202 is: if the terminal device performs the lock screen operation, determining whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time. If the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time, step S206 can be executed; if the virus scan has been performed on the terminal device during the period from the time at which the security software program is installed to the current time, step S203 can be executed.

In one embodiment of the invention, the terminal device can record the time at which the security software program is installed after it may accomplish the installation of the security software program. And then, when the lock screen operation performed by the terminal device is detected, it may be determined whether the virus scan has been performed on the terminal device during the period from the time at which the security software is installed to the current time.

Step S203 is: if determining that the virus scan has been performed on the terminal device during the period from the time at which the security software program is installed to the current time, determining whether the virus scan has been performed on the terminal device during a period from a last time at which a virus database is updated to the current time. If the virus scan has never been performed on the terminal device during the period from the last time at which the virus database is
updated to the current time, step S204 can be executed; if the virus scan has been performed on the terminal device during the period from the last time at which the virus database is updated to the current time, step S205 can be executed.

In one embodiment of the invention, the terminal device can record the last time at which the virus database is updated. Then, when it is determined that the virus scan has been performed during the period from the time at which the security software program is installed to the current time, it may be determined whether the virus scan has been performed during the period from the last time at which the virus database is updated to the current time.

Step S204 is: determining whether a time interval between a last time of virus scanning and the current time is greater than or equal to a first preset time threshold (e.g. 1 day). If the time interval between the last time of virus scanning and the current time is greater than or equal to the first preset time threshold, step S206 can be executed; if the time interval between the last time of virus scanning and the current time is less than the first preset time threshold, the flow may come to the end.

Step S205 is: if determining that the virus scan has been performed on the terminal device during the period from the last time at which the virus database is updated to the current time, determining whether a time interval between a last time of virus scanning and the current time is greater than or equal to a second preset time threshold, wherein the second preset time threshold is greater than the first preset time threshold.

If the time interval between the last time of virus scanning and the current time is greater than or equal to the second preset time threshold, step S206 can be executed; if the time interval between the last time of virus scanning and the current time is less than the second preset time threshold, the flow may come to the end.
In one embodiment of the invention, the terminal device can record the last time of virus scanning. Then, when it is determined that the virus scan has been performed during the period from the last time at which the virus database is updated to the current, it may be determined whether the time interval between the last time of virus scanning and the current is greater than or equal to the second preset time threshold (e.g. 7 days).

Step S206 is: enabling the security software program to perform the virus scan. In one embodiment of the invention, the security software program can also perform the virus scan at the background, which means a security software interface may not need to be enabled. Thus, the consumed resource of the terminal device during the virus scan can be reduced; for example, the terminal device may consume power, etc.

In one embodiment of the invention, the method shown in Fig. 2 can further include: outputting a virus scan result, wherein the virus scan result includes the number of viruses and a prompt message which is used to prompt operations to be performed on a virus, the operations including a clearing operation and an ignoring operation.

When the user selects the clearing operation, the terminal device may clear a detected virus; when the user selects the ignoring operation, the terminal device may ignore the detected virus.

In the method shown in Fig. 2, when the terminal device performs the lock screen operation, it can be taken as a trigger condition. A virus can be scanned in time and the efficiency of virus scanning can be relatively improved.

Referring to Fig. 3, it a structure diagram of an example of a system for scanning virus according to various embodiments. The system can be applied for a terminal device such as a smart phone (e.g., an Android phone, an iOS phone, etc.), a tablet...
computer, a portable computer, a mobile internet device (MID), a personal computer, and so on. The system may include: a monitoring unit 301 configured to monitor whether a terminal device performs a lock screen operation; a first discriminating unit 302 configured to determine whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time, when the monitoring unit 301 detects that the terminal device performs the lock screen operation; and a scan enabling unit 303 configured to enable the security software program to perform the virus scan when the first determining unit 302 determines that the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time.

In the system for virus scanning shown in Fig. 3, when the monitoring unit 301 detects that the terminal device performs the lock screen operation, the first determining unit 302 can determine whether the virus scan has been performed on the terminal device during the period from the time at which the security software program is installed to the current time. If the virus scan has never been performed on the terminal device, the scan enabling unit 303 can enable the security software program to perform the virus scan. In one embodiment of the invention, the terminal device can perform the lock screen operation automatically or under control of the user, which may cause the terminal device performing the lock screen operation frequently. Thus, in the system shown in Fig. 3, when the terminal device performs the lock screen operation, it can be taken as a trigger condition. A virus can be scanned in time and the efficiency of virus scanning can be relatively improved.

Referring to Fig. 4, it is a structure diagram of another example of a system for
scanning virus according to various embodiments. The system shown in Fig. 4 can be obtained by optimizing the system shown in Fig. 3. The system shown in Fig. 4 may include the monitoring unit 301, the first determining unit 302 and the scan enabling unit 303, it may further include: a second determining unit 304 configured to determine whether the virus scan has been performed on the terminal device during a period from a last time at which a virus database is updated to the current time, when the first determining unit 302 determines that the virus scan has been performed on the terminal device during the period from the time at which the security software program is installed to the current time. Correspondingly, the scan enabling unit 303 can be also configured to enable the security software program to perform the virus scan when the second determining unit 304 determines that the virus scan has never been performed on the terminal device during the period from the last time at which the virus database is updated to the current time.

In one embodiment of the invention, the system shown in Fig. 4 may further include: a third determining unit 305 configured to determine whether a time interval between the last time at which the virus database is updated and the current time is greater than or equal to a first preset time threshold, when the second determining unit 304 determines that the virus scan has never been performed on the terminal device during the period from the last time at which the virus database is updated to the current time.

Correspondingly, the scan enabling unit 303 can also be configured to enable the security software program to perform the virus scan when the third determining unit 305 determines that the time interval between the last time at which the virus database is updated and the current time is greater than or equal to the first preset time threshold.
In one embodiment of the invention, the system shown in Fig. 4 further include: a fourth determining unit 306 configured to determine whether a time interval between a last time of virus scanning and the current time is greater than or equal to a second preset time threshold (e.g. 7 days), when the second determining unit determines that the virus scan has been performed on the terminal device during the period from the last time at which the virus database is updated to the current time, wherein the second preset time threshold is greater than the first preset time threshold. Correspondingly, the scan enabling unit 303 can also be configured to enable the security software program to perform the virus scan when the fourth determining unit 306 determines that the time interval between the last time of virus scanning and the current time is greater than or equal to the second preset time threshold.

In one embodiment of the invention, the system shown in Fig. 4 can further include: a recording unit 307 configured to record the time at which the security software program is installed, the last time at which the virus database is updated, and the last time of virus scanning.

In one embodiment of the invention, the system shown in Fig. 4 can further include: an outputting unit 308 configured to output a virus scan result, wherein the virus scan result includes the number of viruses and a prompt message which is used to prompt operations to be performed on a virus, the operations including a clearing operation and an ignoring operation.

In the system shown in Fig. 4, when the terminal device performs the lock screen operation, it can be taken as a trigger condition. A virus can be scanned in time and the efficiency of virus scanning can also be improved.

Referring to Fig. 5, it is a structure diagram of an example of a terminal device.
according to various embodiments. The terminal device can include but not limited to: a smart phone (e.g., an Android phone, an iOS phone, etc.), a tablet computer, a portable computer, a mobile internet device (MID), a personal computer, etc. As shown in Fig. 5, the terminal device may include a system for scanning virus shown in Fig. 3 or Fig. 4. The terminal device can scan a virus in time and also improve the efficiency of virus scanning.

A person having ordinary skills in the art can realize that part or whole of the processes in the methods according to the above embodiments may be implemented by a computer program instructing relevant hardware. The program may be stored in a computer readable storage medium. When executed, the program may execute processes in the above-mentioned embodiments of methods. The storage medium may be a magnetic disk, an optical disk, a Read-Only Memory (ROM), a Random Access Memory (RAM), et al.

The above descriptions are some exemplary embodiments of the invention, and should not be regarded as limitation to the scope of related claims. A person having ordinary skills in a relevant technical field will be able to make improvements and modifications within the spirit of the principle of the invention. The improvements and modifications should also be incorporated in the scope of the claims attached below.
CLAIMS

1. A method for scanning virus, comprising:
   monitoring whether a terminal device performs a lock screen operation;
   determining whether a virus scan has been performed on the terminal device
during a period from a time at which a security software program is installed to a
current time, if the terminal device performs the lock screen operation; and
   enabling the security software program to perform the virus scan, if the virus
scan has never been performed on the terminal device during the period from the time
at which the security software program is installed to the current time.

2. The method of claim 1, further comprising:
   determining whether the virus scan has been performed on the terminal device
during a period from a last time at which a virus database is updated to the current
time, if determining that the virus scan has been performed on the terminal device
during the period from the time at which the security software program is installed to
the current time; and
   enabling the security software program to perform the virus scan, if the virus
scan has never been performed on the terminal device during the period from the last
time at which the virus database is updated to the current time.

3. The method of claim 2, further comprising:
   determining whether a time interval between the last time at which the virus
database is updated and the current time is greater than or equal to a first preset time
threshold, if the virus scan has never been performed on the terminal device during
the period from the last time at which the virus database is updated to the current time;
and

   enabling the security software program to perform the virus scan, if the time
interval between the last time at which the virus database is updated and the current
time is greater than or equal to the first preset time threshold.

4. The method of claim 3, further comprising:

determining whether a time interval between a last time of virus scanning and the
current time is greater than or equal to a second preset time threshold, if determining
that the virus scan has been performed on the terminal device during the period from
the last time at which the virus database is updated to the current time, wherein the
second preset time threshold is greater than the first preset time threshold; and

   enabling the security software program to perform the virus scan, if the time
interval between the last time of virus scanning and the current time is greater than or
equal to the second preset time threshold.

5. The method of claim 4, further comprising:

   recording the time at which the security software program is installed, the last
time at which the virus database is updated, and the last time of virus scanning.

6. The method of any one of claims 1 to 5, further comprising:

   outputting a virus scan result, wherein the virus scan result comprises the number
of viruses and a prompt message configured to prompt operations to be performed on
a virus, the operations comprise a clearing operation and an ignoring operation.
7. A system for scanning virus, comprising:

   a monitoring unit configured to monitor whether a terminal device performs a lock screen operation;

   a first determining unit configured to determine whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time, when the monitoring unit detects that the terminal device performs the lock screen operation; and

   a scan enabling unit configured to enable the security software program to perform the virus scan when the first determining unit determines that the virus scan has never been performed on the terminal device during the period from the time at which the security software program is installed to the current time.

8. The system of claim 7, further comprising:

   a second determining unit configured to determine whether the virus scan has been performed on the terminal device during a period from a last time at which a virus database is updated to the current time, when the first determining unit determines that the virus scan has been performed on the terminal device during the period from the time at which the security software program is installed to the current time;

   wherein the scan enabling unit is also configured to enable the security software program to perform the virus scan when the second determining unit determines that the virus scan has never been performed on the terminal device during the period from the last time at which the virus database is updated to the current time.
9. The system of claim 8, further comprising:

a third determining unit configured to determine whether a time interval between the last time at which the virus database is updated and the current time is greater than or equal to a first preset time threshold, when the second determining unit determines that the virus scan has never been performed on the terminal device during the period from the last time at which the virus database is updated to the current time;

wherein the scan enabling unit is also configured to enable the security software program to perform the virus scan when the third determining unit determines that the time interval between the last time at which the virus database is updated and the current time is greater than or equal to the first preset time threshold.

10. The system of claim 9, further comprising:

a fourth determining unit configured to determine whether a time interval between a last time of virus scanning and the current time is greater than or equal to a second preset time threshold, when the second determining unit determines that the virus scan has been performed on the terminal device during the period from the last time at which the virus database is updated to the current time, wherein the second preset time threshold is greater than the first preset time threshold;

wherein the scan enabling unit is also configured to enable the security software program to perform the virus scan when the fourth determining unit determines that the time interval between the last time of virus scanning and the current time is greater than or equal to the second preset time threshold.
11. The system of claim 10, further comprising:

a recording unit configured to record the time at which the security software program is installed, the last time at which the virus database is updated, and the last time of virus scanning.

12. The system of any one of claims 7 to 11, further comprising:

an outputting unit configured to output a virus scan result, wherein the virus scan result comprises the number of viruses and a prompt message configured to prompt operations to be performed on a virus, the operations comprising a clearing operation and an ignoring operation.

13. A terminal device comprising a system for scanning virus of any one of claims 7-12.
start

monitoring whether a terminal device performs a lock screen operation

no

S101

yes

determining whether a virus scan has been performed on the terminal device during a period from a time at which a security software program is installed to a current time

no

S102

yes

determining whether the virus scan has been performed on the terminal device during a period from a last time at which a virus database is updated to the current time

no

S103

yes

determining whether a time interval between a last time of virus scanning and the current time is greater than or equal to a preset time threshold

no

S104

yes

enabling the security software program to perform the virus scan

S105

end

Fig. 1
Fig. 2
Fig. 3

Fig. 4
virus scanning system

terminal device

Fig. 5
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/14(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DWPLEPODOC,CNPAT,CNKLOGOOGLESCHOLAR:lock+, screen, securit+, idle, device, software, terminal, virus, scan+, automatic+, periodic.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2011239302A1 (SAMSUNG ELECTRONICS CO. LTD.) 29 September 2011 (201 1-09-29) abstract, claims 1-14, description, paragraphs 35-40, figure 1</td>
<td>1-13</td>
</tr>
<tr>
<td>PX</td>
<td>CN 103679022A (TENCENT TECHNOLOGY SHENZHEN CO. LTD.) 26 March 2014 (201W-03-26) abstract, figure 1</td>
<td>1-13</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:
  - "A" document defining the general state of the art which is not considered to be of particular relevance
  - "E" earlier application or patent but published on or after the international filing date
  - "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  - "O" document referring to an oral disclosure, use, exhibition or other means
  - "P" document published prior to the international filing date but later than the priority date claimed
  - "Y" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
  - "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
  - "G" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
  - "P" document member of the same patent family

Date of the actual completion of the international search

12 June 2014

Date of mailing of the international search report

08 July 2014

Name and mailing address of the ISA/
STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA(ISA/CN)
6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088 China

Authorized officer
ZHONG,Hui

Facsimile No. (86-10)62019451

Telephone No. (86-10)62413728

Form PCT/ISA/210 (second sheet) (July 2009)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date (day/month/year)</th>
<th>Patent family member(s)</th>
<th>Publication date (day/month/year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN 103679022A</td>
<td>26 March 2014</td>
<td>WO 2014044109A1</td>
<td>27 March 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2014090062A1</td>
<td>27 March 2014</td>
</tr>
<tr>
<td>US 7231637B1</td>
<td>12 June 2007</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>